UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,831	04/12/2007	Hans Wyssen	27592-01057-US3	4997

30678 7590 01/20/2011

CONNOLLY BOVE LODGE & HUTZ LLP
1875 EYE STREET, N.W.
SUITE 1100
WASHINGTON, DC 20006

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2431	
MAIL DATE	**DELIVERY MODE**
01/20/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/582,831
Filing Date: April 12, 2007
Appellant(s): WYSSEN, HANS

John Paik
Registration No. 54,355
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed November 8, 2010 appealing from the Office action mailed June 8, 2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application: 1-38.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the

subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

6,587,945	PASIEKA	7-2003
7,295,677	SIMPSON	11-2007

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1- 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pasieka (U.S. Patent 6,587,945) in view of Simpson et al. (U.S. Patent 7,295,677).

Regarding claim 1, Pasieka discloses:

A computer system accessible remotely by a user to authenticate a document, comprising:

a memory configured to store electronic image data corresponding to an original document having an electronic displayable verifiable provenance (column 4, lines 13-18: *server stores the image*), and separately derived electronic displayable verification information corresponding to the provenance of at least part of the original document (column 4, lines 49-55: *form an image signature*), and

an output configured to provide said image data and said verification information for display by the user to authenticate the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Pasieka does not explicitly disclose that the verification information is displayed on the image data. In an analogous art, Simpson discloses a visible watermark which is placed on an image which provides authentication information about the user on it (Simpson: column 5, lines 4-16). It would have been obvious to use the visible watermark of Simpson in the system of Pasieka so that the image can still be viewed while still providing information about the owner of the image (Simpson: column 5, lines 5-13).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein the image data has been obtained from an authenticated source, and the verification information includes data corresponding to the provenance of the authenticated source (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein data is fed to and from the memory under the control of a repository (column 4, lines 13-15: *servers signs and stores the image, and then can submit the image to another secure server*).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Pasieka discloses:

A computer system according to claim 3 wherein the verification information comprises data concerning the provenance that has been subjected to authentication by the repository, and the verification information being configured to signal to the user that the repository provides such authentication (column 4, lines 50-55, column 5, lines 4-9: *digital signature of the image to prove the origin*).

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Pasieka discloses:

A computer system according to claim 2 wherein data stored in the memory cannot be altered by users (column 4, lines 48-55: *image is encrypted then stored so it cannot be altered*).

Claim 6 is rejected as applied above in rejecting claim 3. Furthermore, Pasieka discloses:

A computer system according to claim 3 including apparatus to receive the image data from a remote location (column 4, lines 25-30: *server sends image to secure sever over a network*).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 including a scanner for scanning an original document to produce said image data (column 4, lines 15-24: *imager can include a scanner*).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 including a repository agent including apparatus operable to send image data corresponding to an original image to the repository (column 4, lines 25-30: *server sends image to secure sever over a network*).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Pasieka discloses:

A computer system according to claim 8 wherein the repository agent is operable to send the image data together with source authentication information to indicate to the repository that the image data has been sent from the agent (column 4, lines 30-35: *the transmission will identify the author and the imager device*).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein the verification information comprises predetermined accreditation indicia to be viewed by a user concurrently with the image data for authenticating individual parts of the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein the verification information comprises accreditation data to be viewed by a user in a separate field associated with the image data for authenticating the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein the image data and the verification information are stored in a common electronic file (column 4, lines 17-25: *wherein the image can be any file*).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Pasieka discloses:

A computer system according to claim 12 wherein the file is a PDF file (column 4, lines 17-25: *wherein the image can be any file*).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 including a server providing said memory and operable to host a website at which said image data and verification information is viewable by a user to authenticate the original document (column 5, lines 55-67: *wherein a server is used to view the images, and wherein it is inherent that the server can act like a web server*).

Claim 15 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein said output is connected to the Internet (column 4, lines 27-29: *image can be sent over a public network*).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses;

A computer system according to claim 1 wherein said image data and verification information in the memory is password protected so that the user can only gain access

thereto by use of the password (column 5, lines 10-13: *wherein there are different password pairs*).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A computer system according to claim 1 wherein the image data and the verification information corresponding to the original document when stored in the memory collectively has an individual addressable identity (column 4, lines 31-35: *image record stored with an image ID*).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Pasieka discloses:

A method of operating a computer system according to claim 1 to provide said image data and said verification information for display by the user to authenticate the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Regarding claim 19, Pasieka discloses:

A method of displaying a document for authentication, comprising:

creating electronic image data corresponding to an original document having an electronic displayable verifiable provenance (column 4, lines 15-24: *imager can include a scanner*),

providing electronic, displayable verification information corresponding to the provenance of at least part of the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*), and

displaying the image data and the verification information, to permit a user to authenticate the document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Pasieka does not explicitly disclose that the verification information is displayed on the image data. In an analogous art, Simpson discloses a visible watermark which is placed on an image which provides authentication information about the user on it (Simpson: column 5, lines 4-16). It would have been obvious to use the visible watermark of Simpson in the system of Pasieka so that the image can still be viewed while still providing information about the owner of the image (Simpson: column 5, lines 5-13).

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Pasieka discloses:

A method according to claim 19 including receiving the image data from an authenticated source (column 5, lines 55-65: *image, origin, integrity are displayed to a user*), storing the image data for display (column 4, lines 13-18: *server stores the image*), and creating the verification information for the received image (column 4, lines 49-55: *form an image signature*), wherein the verification information includes data

corresponding to the provenance of the authenticated source (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 21 is rejected as applied above in rejecting claim 19. Furthermore, Pasieka discloses:

A method according to claim 19 including authenticating the source of the image data (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 22 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 including feeding the image data and the verification information to a memory under the control of a repository for display to users wishing to authenticate the original document (column 4, lines 13-15: *servers signs and stores the image, and then can submit the image to another secure server*).

Claim 23 is rejected as applied above in rejecting claim 22. Furthermore, Pasieka discloses:

A method according to claim 22 wherein only the repository can change the data in the memory (column 4, lines 48-55: *image is encrypted then stored so it cannot be altered*).

Claim 24 is rejected as applied above in rejecting claim 22. Furthermore, Pasieka discloses:

A method according to claim 22 wherein the verification information comprises data concerning the provenance that has been authenticated by the repository (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Pasieka discloses:

A method according to claim 24 wherein the repository communicates with the source of the image data to determine the provenance thereof and to develop said verification information (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 26 is rejected as applied above in rejecting claim 22. Furthermore, Pasieka discloses:

A method according to claim 22 including feeding the image data to the repository from a remote location (column 4, lines 25-30: *server sends image to secure sever over a network*).

Claim 27 is rejected as applied above in rejecting claim 22. Furthermore, Pasieka discloses:

A method according to claim 22 including sending send image data corresponding to an original image from a repository agent to the repository (column 4, lines 12-15: *image is originally sent to a server which signs and stores it*).

Claim 28 is rejected as applied above in rejecting claim 26. Furthermore, Pasieka discloses:

A method according to claim 26 including sending the image data together with source authentication information to indicate to the repository that the image data has been sent from the repository agent (column 4, lines 30-35: *the transmission will identify the author and the imager device*).

Claim 29 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 including configuring the verification information to include predetermined accreditation indicia viewable concurrently with the image data for authenticating individual parts of the original document by a user that authenticates the document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 30 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 including configuring the verification information to comprise accreditation data to be viewable by a user in a separate field associated

with the image data for authenticating the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 31 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 including storing the image data and the verification information are stored in a common electronic file (column 4, lines 17-25: *wherein the image can be any file*).

Claim 32 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 including storing the image data and the verification information are stored in a common electronic PDF file (column 4, lines 17-25: *wherein the image can be any file*).

Claim 33 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 including hosting a website at which said image data and verification information is viewable by a user to authenticate the original document (column 5, lines 55-67: *wherein a server is used to view the images, and wherein it is inherent that the server can act like a web server*).

Claim 34 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 including authenticating the original document by viewing said electronic image data and the corresponding verification information (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Claim 35 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses;

A method according to claim 18 wherein said image data and verification information is password protected so that a user can only gain access thereto by use of the password, and including supplying the password to a user to permit the user to authenticate the original document (column 5, lines 10-13: *wherein there are different password pairs*).

Claim 36 is rejected as applied above in rejecting claim 18. Furthermore, Pasieka discloses:

A method according to claim 18 wherein the image data and the verification information corresponding to the original document collectively have an individual addressable identity and including supplying the individual addressable identity to a user to permit the user to access the data and information for authenticating the original document (column 4, lines 31-35: *image record stored with an image ID*).

Claim 37 is rejected as applied above in rejecting claim 35. Furthermore, Pasieka discloses:

A method according to claim 35 including supplying a hyperlink to the user (column 5, lines 10-13: *wherein there are different password pairs, and it is well-known to supply information via hyperlinks*)

Regarding claim 38, Pasieka discloses:

A computer system comprising:

a unit for processing an electrical signal for displaying a document for authentication to be received by a client computer operated by a user who wishes to authenticate the document (column 4, lines 10-40), wherein the electronic signal comprises:

an electronic image data corresponding to an original document having a verifiable provenance (column 4, lines 13-18: *server stores the image*), and

electronic, displayable verification information corresponding to the provenance of at least part of the original document (column 5, lines 55-65: *image, origin, integrity are displayed to a user*).

Pasieka does not explicitly disclose that the verification information is displayed on the image data. In an analogous art, Simpson discloses a visible watermark which is placed on an image which provides authentication information about the user on it (Simpson: column 5, lines 4-16). It would have been obvious to use the visible watermark of Simpson in the system of Pasieka so that the image can still be viewed

while still providing information about the owner of the image (Simpson: column 5, lines 5-13).

(10) Response to Argument

Argument A.I: Pasieka and Simpson fail in Any Combination to Teach or Suggest at least the recited "original tangible document...having an electronic displayable verifiable provenance" of Claim 1.

The Appellant argues that Pasieka does not teach an original tangible document having an electronic displayable verifiable provenance.

The Examiner contends that Pasieka does teach an original tangible document having an electronic displayable verifiable provenance. First, the Examiner would like to note that the word "tangible" is not defined in the specification in such a way to limit a document to only a paper document. If tangible is given its broadest reasonable interpretation according to the Merriam-Webster dictionary it would be anything that is capable of being perceived. Under this definition, a document that is created on an electronic document would be "tangible" as it is capable of being perceived and it is displayed. Using this argument, Pasieka discloses an embodiment where an author creates a document which contains an author's ID (column 8, lines 30-35). The author's ID is an electronic displayable verifiable provenance as it is used to form an image record (document) which is used to verify the author and origin of the document (column 5, lines 55-60). Alternatively, even if the document is a paper copy, the Examiner contends that Pasieka still teaches an original tangible document having an electronic

displayable verifiable provenance. Pasieka teaches an imager that is used to create an image wherein the imager includes a fax machine or scanner where the paper document are scanned in and converted to a digital form (column 4, lines 11-20). These papers include contracts which contain signatures of the contractors (provenance) (column 8, lines 24-30) that will appear unaltered in a scanned image. This scanned document along with an origin id can be displayed to a reviewer to verify if it is signed (column 5, lines 55-62). Therefore, the Examiner contends that Pasieka does teach an original tangible document having an electronic displayable verifiable provenance.

Argument A.II: Pasieka and Simpson fail in Any Combination to Teach or Suggest at least the recited "separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance" of Claim 1.

The Appellant further argues that Pasieka and Simpson in any combination do not teach "separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance."

The Examiner contends that Pasieka teaches separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance. The image which can be a scanned contract (column 8, lines 24-30) or created (column 4, lines 16-22) contains an origin ID which is displayed to a reviewer

(column 5, lines 55-62). This document containing the ID or signature field is made into a document record which is then hashed to provide an image fingerprint (column 4, lines 40-50). This image fingerprint, which is a separately derived displayable verification information related to the document and thus the provenance, is then compared to an image fingerprint generated by a display to verify if the image is authentic (column 6, lines 1-14) to a reviewer. Therefore, the Examiner contends that Pasieka does teach separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance.

Argument B: Pasieka and Simpson fail to teach in any combination the recited elements of claims 19-37.

The Appellant further argues that Pasieka and Simpson in any combination fail to teach or suggest the recited elements in claims 19-37, including the original document having an electronic verifiable provenance and displayable verification information corresponding to the electronic displayable provenance.

The Examiner contends that Pasieka does teach an original tangible document having an electronic displayable verifiable provenance. First, the Examiner would like to note that the word "tangible" is not defined in the specification in such a way to limit a document to only a paper document. If tangible is given its broadest reasonable interpretation according to the Merriam-Webster dictionary it would be anything that is capable of being perceived. Under this definition, a document that is created on an

electronic document would be “tangible" as it is capable of being perceived and it is displayed. Using this argument, Pasieka discloses an embodiment where an author creates a document which contains an author's ID (column 8, lines 30-35). The author's ID is an electronic displayable verifiable provenance as it is used to form an image record (document) which is used to verify the author and origin of the document (column 5, lines 55-60). Alternatively, even if the document is a paper copy, the Examiner contends that Pasieka still teaches an original tangible document having an electronic displayable verifiable provenance. Pasieka teaches an imager that is used to create an image wherein the imager includes a fax machine or scanner where the paper document are scanned in and converted to a digital form (column 4, lines 11-20). These papers include contracts which contain signatures of the contractors (provenance) (column 8, lines 24-30) that will appear unaltered in a scanned image. This scanned document along with an origin id can be displayed to a reviewer to verify if it is signed (column 5, lines 55-62). Therefore, the Examiner contends that Pasieka does teach an original tangible document having an electronic displayable verifiable provenance.

Furthermore, the Examiner contends that Pasieka teaches separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance. The image which can be a scanned contract (column 8, lines 24-30) or created (column 4, lines 16-22) contains an origin ID which is displayed to a reviewer (column 5, lines 55-62). This document containing the ID or signature field is made into a document record which is then hashed to provide an

image fingerprint (column 4, lines 40-50). This image fingerprint, which is a separately derived displayable verification information related to the document and thus the provenance, is then compared to an image fingerprint generated by a display to verify if the image is authentic (column 6, lines 1-14) to a reviewer. Therefore, the Examiner contends that Pasieka does teach separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance.

Argument C: Pasieka and Simpson fail to teach in any combination the recited elements of claims 38.

The Appellant finally argues that Pasieka and Simpson in any combination fail to teach or suggest the recited elements in claims 19-37, including the original document having an electronic verifiable provenance and displayable verification information corresponding to the electronic displayable provenance.

The Examiner contends that Pasieka does teach an original tangible document having an electronic displayable verifiable provenance. First, the Examiner would like to note that the word "tangible" is not defined in the specification in such a way to limit a document to only a paper document. If tangible is given its broadest reasonable interpretation according to the Merriam-Webster dictionary it would be anything that is capable of being perceived. Under this definition, a document that is created on an electronic document would be "tangible" as it is capable of being perceived and it is displayed. Using this argument, Pasieka discloses an embodiment where an author

creates a document which contains an author's ID (column 8, lines 30-35). The author's ID is an electronic displayable verifiable provenance as it is used to form an image record (document) which is used to verify the author and origin of the document (column 5, lines 55-60). Alternatively, even if the document is a paper copy, the Examiner contends that Pasieka still teaches an original tangible document having an electronic displayable verifiable provenance. Pasieka teaches an imager that is used to create an image wherein the imager includes a fax machine or scanner where the paper document are scanned in and converted to a digital form (column 4, lines 11-20). These papers include contracts which contain signatures of the contractors (provenance) (column 8, lines 24-30) that will appear unaltered in a scanned image. This scanned document along with an origin id can be displayed to a reviewer to verify if it is signed (column 5, lines 55-62). Therefore, the Examiner contends that Pasieka does teach an original tangible document having an electronic displayable verifiable provenance.

Furthermore, the Examiner contends that Pasieka teaches separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance. The image which can be a scanned contract (column 8, lines 24-30) or created (column 4, lines 16-22) contains an origin ID which is displayed to a reviewer (column 5, lines 55-62). This document containing the ID or signature field is made into a document record which is then hashed to provide an image fingerprint (column 4, lines 40-50). This image fingerprint, which is a separately derived displayable verification information related to the document and thus the

provenance, is then compared to an image fingerprint generated by a display to verify if the image is authentic (column 6, lines 1-14) to a reviewer. Therefore, the Examiner contends that Pasieka does teach separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Kaveh Abrishamkar/

Primary Examiner, Art Unit 2431

Conferees:

/Christopher A. Revak/

Primary Examiner, Art Unit 2431

/saleh najjar/

Supervisory Patent Examiner, Art Unit 2455